

Requested Patent: JP62241061A
Title: INFORMATION ACCESS MANAGEMENT SYSTEM ;
Abstracted Patent: JP62241061 ;
Publication Date: 1987-10-21 ;
Inventor(s): SHIMOSATO MASAO ;
Applicant(s): NEC CORP ;
Application Number: JP19860083842 19860411 ;
Priority Number(s): ;
IPC Classification: G06F15/16; G06F12/00 ;
Equivalents: ;

ABSTRACT:

PURPOSE: To eliminate the need for changing access rights for reference and updating required for each change in constituent members, by registering not only the names of the users who can refer to and update the information stored in a file area but also their hierarchical positions, etc.

CONSTITUTION: A register means 1 registers the access right management information including the accessible hierarchy information showing the hierarchical positions of the users who can refer to and update the information stored in a file and the file name and then stores the information in an access right memory means 2. A request accepting means 4 accepts file access requests for reference/updating of the information stored in the file from users and judges these request via a deciding means 3 based on user organization information informed via an organization information transmitting means 6 and the access right management information stored in the means 2. Based on the judgement result of the means 3, the permission or rejection of the file access request is informed in reply to the user who had file access through an answer means 5.

⑫ 公開特許公報(A)

昭62-241061

⑤ Int.Cl.⁴G 06 F 15/16
12/00

識別記号

3 0 2

庁内整理番号

Z-2116-5B
6711-5B

④ 公開 昭和62年(1987)10月21日

審査請求 未請求 発明の数 1 (全7頁)

⑬ 発明の名称 情報アクセス管理方式

⑰ 特 願 昭61-83842

⑱ 出 願 昭61(1986)4月11日

⑭ 発 明 者 下 郷 昌 夫 東京都港区芝5丁目33番1号 日本電気株式会社内
⑯ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号
⑰ 代 理 人 弁理士 河原 純一

明 細 書

1. 発明の名称

情報アクセス管理方式

2. 特許請求の範囲

単一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおいて、

前記電子計算機システムのファイルに格納されている情報を参照、更新ないしは参照および更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報と前記情報が格納されているファイルを識別するファイル名とから構成されるアクセス権管理情報を登録する登録手段と、

この登録手段から供給される前記アクセス権管理情報を記憶するアクセス権記憶手段と、

前記電子計算機システムの利用者からのファイ

ルに格納されている情報を参照ないしは更新するファイルアクセス要求を受け付ける要求受け手段と、

前記電子計算機システムの利用者の利用者と利用者の組織階層の階層位置情報とで構成される利用者組織情報を通知する組織情報通知手段と、

前記要求受け手段から供給される前記ファイルアクセス要求の正当性を前記組織情報通知手段によって通知される前記利用者組織情報と前記アクセス権記憶手段によって記憶されている前記アクセス権管理情報とに基づいて判定する判定手段と、

この判定手段からの判定結果に基づき前記ファイルアクセス要求の許可ないしは拒否をファイルアクセスを要求した前記利用者に応答する応答手段と、

を含むことを特徴とする情報アクセス管理方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は情報アクセス管理方式に関し、特に単

一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上のファイルに格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおける情報アクセス管理方式に関する。

(従来の技術)

不特定多数の利用者により利用される単一ないしはネットワークで結ばれた複数の電子計算機システムにおいては、電子計算機システム内の情報を第三者の参照ないしは更新から保護することが必要である。

従来、電子計算機システムにおいて、情報は主記憶装置ないしは補助記憶装置上に確保されたファイルと呼ばれる領域に格納され、第三者からの情報の参照ないしは更新の保護管理は情報が格納されているファイルへのアクセス権として管理され、各ファイルごとにアクセス権を持つ単一ないしはネットワークで結ばれた複数の電子計算機システムの利用者の一人ないしは複数の利用者を

来技術によって実現されるが、情報を参照ないしは更新する利用者が少なく情報と情報を参照ないしは更新する利用者との関係が長期間固定しているような場合には余り問題にはならないが、情報を参照ないしは更新する利用者数が多いと情報が格納されているファイルに対応したファイルへのアクセス権を持つ利用者数が非常に多くなり、また情報と情報を参照ないしは更新する利用者との関係が度々変わるような場合には、情報と情報を参照ないしは更新する利用者との関係が変わるごとに影響をうける各ファイルすべてのファイルへのアクセス権を持つ利用者名を変更しなければならないという欠点がある。

⑤のレベルは、複数の利用者名を指定せしめることにより従来技術でも実現されえないことはないが、利用者数が多いと情報が格納されているファイルに対応したファイルへのアクセス権を持つ利用者数が多いと非常に多くなり、また情報と情報を参照ないしは更新する利用者との関係が度々変わるような場合には、情報と情報を参照ないしは更新

指定せしめ、指定されていない利用者がファイルにアクセスすることを拒絶することにより、主記憶装置ないしは補助記憶装置上に格納されている情報を第三者の参照ないしは更新から保護している。

(発明が解決しようとする問題点)

不特定多数の利用者により利用される単一ないしはネットワークで結ばれた複数の電子計算機システムのファイル内に格納されている情報を複数の利用者間で参照ないしは更新する利用形態において、ファイルにアクセスできる利用者の範囲は、

- ① 範囲を限定しない、
- ② 特定個人に限定、
- ③ 複数人に限定

の3レベルに分類される。

①のレベルは、誰でもがアクセスできるレベルであるので、誰でもアクセス可能と指定せしめることにより従来技術によって実現されうる。

②のレベルは、ファイルごとにファイルをアクセスできる利用者名を設定せしめることにより従

する利用者との関係が変わるごとに影響をうける各ファイルすべてのファイルへのアクセス権を持つ利用者名を変更しなければならないという欠点がある。

多数の利用者で情報を参照ないしは更新するのは、たとえば会社などの階層的組織がほとんどである。会社などの階層的組織では、組織内での階層位置ないしは階層の上下関係により情報へのアクセス権が決まり、各個人が誰であるかは問われない情報と個人のみで参照ないしは更新する情報とが大部分であり、特定の複数者のみ参照ないしは更新する情報は少ない。

本発明の目的は、上述の点に鑑み、階層的組織では組織内のかなりの情報が組織内での階層位置ないしは階層の上下関係により情報へのアクセス権が決まり各個人が誰であるかは問われない性格を持っていることに着目して、階層的組織の構成員の変動の度ごとに各情報が格納されているファイルの参照ないしは更新のためのアクセス権を変更する必要のない情報アクセス管理方式を提供す

ることにある。

(問題点を解決するための手段)

本発明の情報アクセス管理方式は、単一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおいて、前記電子計算機システムのファイルに格納されている情報を参照、更新ないしは参照および更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報と前記情報が格納されているファイルを識別するファイル名とから構成されるアクセス権管理情報を登録する登録手段と、この登録手段から供給される前記アクセス権管理情報を記憶するアクセス権記憶手段と、前記電子計算機システムの利用者からのファイルに格納されている情報を参照ないしは更新するファイルアクセス要求を受け付ける要求受け手段と、前記電子計算機システムの利用者

ップ21および登録情報通知ステップ22からなる。

第3図を参照すると、アクセス権記憶手段2における処理は、登録情報受け付けステップ31および登録情報記憶ステップ32からなる。

第4図を参照すると、判定手段3における処理は、ファイルアクセス要求情報受け付けステップ41、アクセス権情報取得ステップ42、組織情報取得ステップ43、正当性判定ステップ44、正当通知ステップ45および不当通知ステップ46からなる。

第5図を参照すると、要求受け手段4における処理は、ファイルアクセス要求受け付けステップ51およびファイルアクセス要求情報通知ステップ52からなる。

第6図を参照すると、応答手段5における処理は、判定結果取得ステップ61、判定結果比較ステップ62、要求許可通知ステップ63および要求拒否通知ステップ64からなる。

第7図を参照すると、組織情報通知手段6にお

の利用者名と利用者の組織階層の階層位置情報とで構成される利用者組織情報を通知する組織情報通知手段と、前記要求受け手段から供給される前記ファイルアクセス要求の正当性を前記組織情報通知手段によって通知される前記利用者組織情報と前記アクセス権記憶手段によって記憶されている前記アクセス権管理情報とに基づいて判定する判定手段と、この判定手段からの判定結果に基づき前記ファイルアクセス要求の許可ないしは拒否をファイルアクセスを要求した前記利用者に応答する応答手段とを含む。

(実施例)

次に、本発明について図面を参照して詳細に説明する。

第1図を参照すると、本発明の一実施例は、登録手段1、アクセス権記憶手段2、判定手段3、要求受け手段4、応答手段5および組織情報通知手段6から構成されている。

第2図を参照すると、登録手段1における処理は、ファイルアクセス権情報登録要求受けステ

における処理は、取得要求受けステップ71、組織情報取得ステップ72および組織情報通知ステップ73からなる。

第8図を参照すると、アクセス権管理情報80は、ファイルを識別するファイル名81と、そのファイルに格納されている情報を参照ないしは更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報82とから構成されている。

第9図を参照すると、利用者組織情報90は、利用者の利用者名91と、利用者の組織階層の階層位置情報92とから構成されている。

ここで、組織の階層位置とは、会社の部とか課とか研究所のグループなどの防層的な組織の組織単位であり、上下位置関係とは、その階層の課長とか部長とかグループ長などの役職の上下関係のことである。

次に、このように構成された本実施例の情報アクセス管理方式の動作について説明する。

まず、利用者は、情報を作成すると、作成した

情報を格納するファイルを電子計算機システムの主記憶ないしは補助記憶装置上に確保して情報を格納する。このとき、利用者は、情報を格納したファイル名81に対応して格納情報を参照ないしは更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報82を指定して登録手段1を動作させる。

登録手段1は、ファイルアクセス権情報登録要求受け付けステップ21でこの登録要求を受け付け、登録情報通知ステップ22でこの登録情報をアクセス権記憶手段2に通知する。

アクセス権記憶手段2は、この登録情報を登録情報受け付けステップ31で受け付け、登録情報記憶ステップ32でこの登録情報であるアクセス可能階層情報82と作成した情報を格納したファイルを識別するファイル名81とがアクセス権管理情報として記憶されて動作が停止される。

次に、利用者は、ファイルに格納されている情報を参照ないしは更新するというファイルアクセス要求を行い、要求受け付け手段4を動作させる。

73で判定手段3に通知する。

判定手段3は、この通知された利用者組織情報90を組織情報取得ステップ43で取得し、この利用者組織情報90とアクセス権管理情報80とから正当性判定ステップ44で利用者のファイルアクセス要求の正当性が判定される。この判定結果が正当であれば、正当通知ステップ45で正当という判定結果が応答手段5に通知される。判定結果が不当であれば、不当通知ステップ46で不当という判定結果が応答手段5に通知される。

応答手段5は、この判定結果通知を判定結果取得ステップ61で取得し、判定結果比較ステップ62で取得された判定結果が正当であるか不当であるかを比較によって判定し、比較結果が正当であれば要求許可通知ステップ63で利用者に許可が通知されて動作が停止される。比較結果が不当であれば、要求拒否通知ステップ64で利用者に拒否が通知されて動作が停止される。

次に、判定手段3における判定処理について具体例を用いて説明する。ここでは、第10図(a)

要求受け付け手段4は、このファイルアクセス要求をファイルアクセス要求受け付けステップ51で受け付け、ファイルアクセス要求情報通知ステップ52で参照ないしは更新要求するファイル名と要求利用者名とで構成されるファイルアクセス要求情報を判定手段3に通知する。

判定手段3は、このファイルアクセス要求情報の通知をファイルアクセス要求情報受け付けステップ41で受け付け、アクセス権情報取得ステップ42でこの受け付けたファイルアクセス要求情報のファイル名に対応するファイルのアクセス権記憶手段2によって記憶されたアクセス権管理情報80が取得され、さらに組織情報取得ステップ43でファイルアクセス要求情報の利用者名に対応する利用者の利用者組織情報90を通知するように組織情報通知手段6に要求する。

組織情報通知手段6は、この要求を取得要求受け付けステップ71で受け付け、組織情報取得ステップ72で要求された利用者名に対応する利用者組織情報90を取得し、組織情報通知ステップ

で示される階層の組織において、第10図(b)で示されるアクセス可能階層情報82が登録されているファイルに格納されている情報をアクセスする場合を例にとって説明する。

第10図(a)は、組織階層の一例を示し、A～A a a a c bはその組織の階層位置を示す。

第10図(b)は、ファイルに対応したアクセス可能階層情報82の一例を示す。

第10図(c)は、第10図(a)で示される組織において、第10図(b)で示されるアクセス可能階層情報が登録されているファイルにアクセスできる階層位置のリストを示す。ここで、参照可能階層位置リストのA a a a a、A a a a b、A a a a cおよびA a a a dは、第10図(b)の参照アクセス可能階層情報の同階層という登録情報から、A a a aおよびA a aは直上2階層までという登録情報から、A a a bおよびA a a cは直上2階層下の直下1階層という登録情報からそれぞれ導かれる。また、更新可能階層位置リストのA a a aは、第10図(b)の更新アクセス

可能階層情報の直上1階層という登録情報から導かれる。

例えば、A a a a aの階層位置の利用者のファイルに格納されている情報への参照アクセス要求は、第10図(c)に示される参照可能階層位置リストに利用者のA a a a aという階層位置が含まれているので正当と判定されるが、更新アクセス要求は第10図(c)に示される更新可能階層位置リストにA a a a aという階層位置が含まれていないので不当と判定される。また、A a a aの階層位置の利用者の参照アクセス要求は、第10図(c)に示される参照可能階層位置リストに利用者のA a a a aという階層位置が含まれているので正当と判定され、更新アクセス要求も第10図(c)に示される更新可能階層位置リストにA a a a aという階層位置が含まれているので正当と判定される。

しかしながら、A a a a c aやA a bなどの階層位置の利用者の参照アクセス要求ないしは更新アクセス要求は、第10図(c)に示される参照

可能階層位置リストにも更新可能階層位置リストにもA a a a c aおよびA a bという階層位置は含まれていないので、両方とも不当と判定される。

(発明の効果)

以上説明したように本発明には、主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新できる1人ないしは複数の利用者名だけでなく、組織階層の階層位置ないしは上下位置関係を各ファイルに対して登録できるようにすることにより、単一ないしはネットワークで結ばれた複数の電子計算機システムの情報を複数の利用者で参照ないしは更新する利用形態において、組織構成員が絶えず変動しても、組織階層の階層位置ないしは上下位置関係を指定されたファイルにおいては、ファイルへのアクセス権はアクセス要求者の組織階層の階層位置ないしは上下位置関係により決まり、要求者個人の利用者名には依存しないので、構成員の変動の度ごとに各情報が格納されているファイルの参照ないしは更新のための

アクセス権を変更する必要がなくなるという効果がある。

4. 図面の簡単な説明

第1図は本発明の一実施例を示す構成図、

第2図は第1図中に示した登録手段における処理を示す流れ図、

第3図は第1図中に示したアクセス権記憶手段における処理を示す流れ図、

第4図は第1図中に示した判定手段における処理を示す流れ図、

第5図は第1図中に示した要求受け手段における処理を示す流れ図、

第6図は第1図中に示した応答手段における処理を示す流れ図、

第7図は第1図中に示した組織情報通知手段における処理を示す流れ図、

第8図はアクセス権管理情報の構成を示す図、

第9図は利用者組織情報の構成を示す図、

第10図(a)～(c)は階層組織の一例を示す図、アクセス可能階層情報を示す図およびアク

セス可能階層位置のリストである。

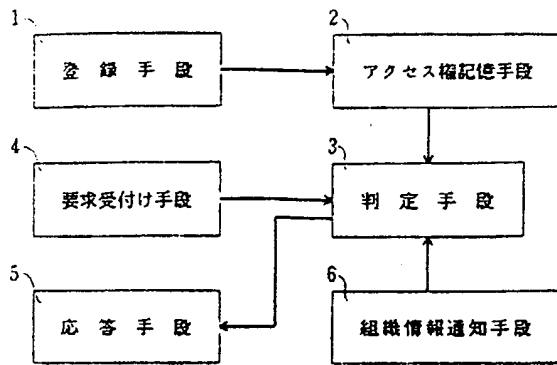
図において、

- 1・・・登録手段、
- 2・・・アクセス権記憶手段、
- 3・・・判定手段、
- 4・・・要求受け手段、
- 5・・・応答手段、
- 6・・・組織情報通知手段である。

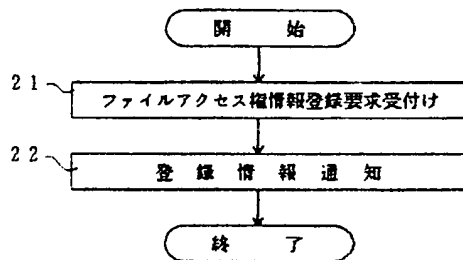
特許出願人 日本電気株式会社

代理人 弁理士 河原 純 一

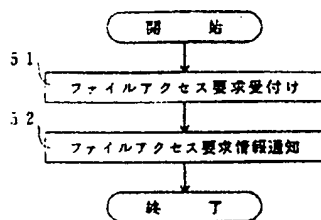
第 1 図



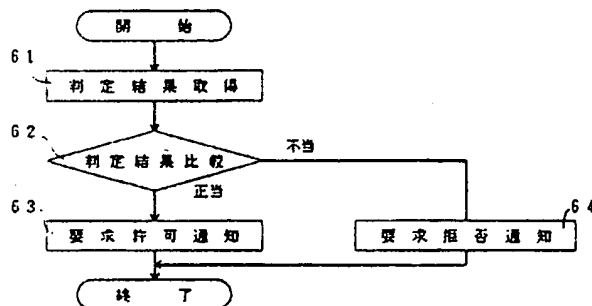
第 2 図



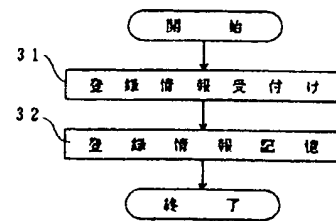
第 5 図



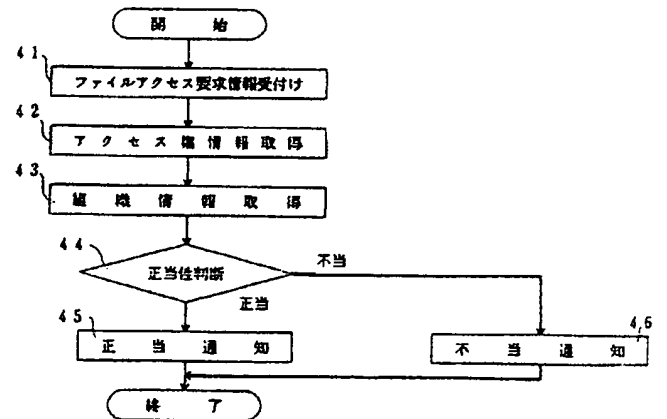
第 6 図



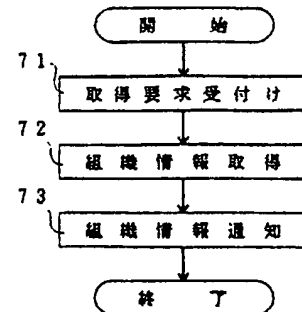
第 3 図



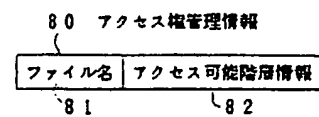
第 4 図



第 7 図



第 8 図



第 9 図

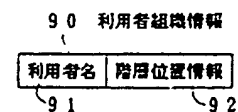


図 10 (a)

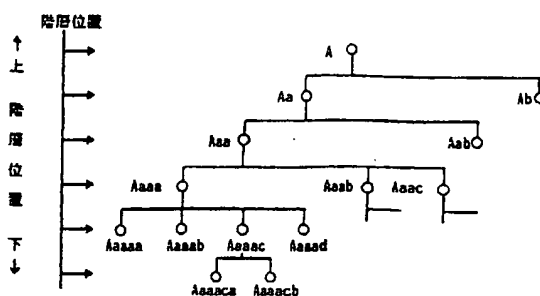


図 10 (b)

	登録情報
階層基準階層位置	Aaaaab
参照アクセス可能階層	同階層、直上2階層まで、直上2階層下の直下1階層
更新アクセス可能階層	直上1階層

図 10 (c)

アクセス種類	アクセス可能階層位置リスト
参照	Aaaaa, Aaaaab, Aaaac, Aaaad, Aaaa, Aaa, Aaab, Aaac
更新	Aaaa